CLAIMS

1. A method for releasing digital content to a rendering application, the rendering application for forwarding the digital content to an ultimate destination by way of a path therebetween, the path being defined by at least one module, the digital content initially being in an encrypted form, the method comprising:

performing an authentication of at least a portion of the path to determine whether each defining module thereof is to be trusted to appropriately handle the digital content passing therethrough;

decrypting the encrypted digital content if in fact each such defining module is to be trusted; and

forwarding the decrypted digital content to the rendering application for further forwarding to the ultimate destination by way of the authenticated path.

2. The method of claim 1 wherein the path includes a user mode portion and a kernel portion, the method further comprising:

scrambling the digital content upon such digital content being outputted from the rendering application to the path such that the scrambled digital content enters the user mode portion of the path, such scrambled digital content then passing through the modules that define the user mode portion of the path and transiting from the user mode portion to the kernel portion of the path; and

de-scrambling the scrambled digital content upon such scrambled digital content transiting from the user mode portion to the kernel portion.

3. The method of claim 2 comprising de-scrambling the scrambled digital content by way of a de-scrambling module.

4. The method of claim 2 comprising de-scrambling the scrambled digital content in the kernel portion of the path.

5. The method of claim 4 comprising performing an authentication of at least a portion of the kernel portion of the path to determine whether each defining module thereof is to be trusted to appropriately handle the digital content passing therethrough.

6. The method of claim 1 wherein the path includes a user mode portion and a kernel portion, the method comprising performing an authentication of at least a portion of the kernel portion of the path to determine whether each defining module thereof is to be trusted to appropriately handle the digital content passing therethrough.

7. The method of claim 6 further comprising:

scrambling the digital content upon such digital content being outputted from the rendering application to the path such that the scrambled digital content enters the user mode portion of the path, such scrambled digital content then passing through the modules that define the user mode portion of the path and transiting from the user mode portion to the kernel portion of the path; and

de-scrambling the scrambled digital content upon such scrambled digital content transiting from the user mode portion to the kernel portion.

8. The method of claim 7 comprising de-scrambling the scrambled digital content by way of a de-scrambling module.

9. The method of claim 7 comprising de-scrambling the scrambled digital content in the kernel portion of the path.

10. The method of claim 1 wherein performing the authentication comprises:

traversing the at least a portion of the path to develop a map of each module in the path; and

authenticating each module in the map.

11. The method of claim 10 wherein performing the authentication further comprises ignoring each module not in the map.

12. The method of claim 1 wherein performing the authentication comprises:

authenticating an initial module;

determining all first destination modules that receive data from such initial module;

authenticating each such first destination module;

determining all second destination modules that receive data from each such first destination module;

iteratively repeating the authenticating and determining steps for third, fourth, fifth, etc. destination modules until each module in such at least a portion of the path has been determined and authenticated.

13. The method of claim 12 wherein authenticating the initial module comprises authenticating a module in the at least a portion of the path that is to receive the digital content before any other module in the at least a portion of the path, whereby the initial module leads to fully determining all other modules that define the at least a portion of the path.

14. The method of claim 12 comprising employing a database device to keep track of all modules determined to be in the at least a portion of the path, whereby already-determined modules in the at least a portion of the path can be recognized.

15. The method of claim 1 wherein performing an authentication

comprises:

for each module in the at least a portion of the path:

receiving from the module a certificate as issued by a certifying authority; and

determining from the received certificate whether such received certificate is acceptable for purposes of authenticating the module.

16. The method of claim 15 wherein performing an authentication further comprises checking a revocation list to ensure that the received certificate has not been revoked.

17. The method of claim 16 further comprising:

receiving the revocation list from a certifying authority;

storing the received revocation list in a secure location.

18. The method of claim 15 wherein performing an authentication further comprises refusing to decrypt the encrypted digital content if at least one module in the at least a portion of the path fails to provide an acceptable certificate.

19. The method of claim 15 wherein performing an authentication further comprises decrypting the encrypted digital content if all the modules in the at least a portion of the path provide an acceptable certificate.

20. The method of claim 15 wherein performing an authentication further comprises, for each module in the at least a portion of the path that fails to provide an acceptable certificate:

defining a sub-portion of the path including the non-providing module;

scrambling the digital content upon such digital content entering the sub-portion of the path, such scrambled digital content then passing through the modules

that define the sub-portion of the path; and

de-scrambling the scrambled digital content upon such scrambled digital content exiting from the sub-portion of the path; and

declaring the sub-portion trustworthy.

21. The method of claim 1 wherein the path includes a user mode portion and a kernel portion, the method comprising performing an authentication of the user mode portion of the path and of the kernel portion of the path to determine whether each defining module thereof is to be trusted to appropriately handle the digital content passing therethrough.

22. The method of claim 1 wherein the path includes a tunneled portion, the method further comprising:

scrambling the digital content upon such digital content entering the tunneled portion of the path, such scrambled digital content then passing through the modules that define the tunneled portion of the path; and

de-scrambling the scrambled digital content upon such scrambled digital content exiting from the tunneled portion of the path;

and wherein performing an authentication comprises performing an authentication of at least a portion of the path external to the tunneled portion of the path to determine whether each defining module thereof is to be trusted to appropriately handle the digital content passing therethrough, an authentication of the tunneled portion being unnecessary.

23. The method of claim 22 wherein the path includes a user mode portion, a kernel portion, and a tunneled portion in the user mode portion, the method further comprising:

scrambling the digital content upon such digital content entering the tunneled portion of the user mode portion of the path, such scrambled digital content then passing through the modules that define the tunneled portion of the user mode portion of

the path; and

de-scrambling the scrambled digital content upon such scrambled digital content exiting from the tunneled portion of the user mode portion of the path.

and wherein performing an authentication comprises performing an authentication of at least a portion of the path external to the tunneled portion of the user mode portion of the path to determine whether each defining module thereof is to be trusted to appropriately handle the digital content passing therethrough, an authentication of the tunneled portion being unnecessary.

24. A computer-readable medium having computer-executable instructions thereon for performing a method for releasing digital content to a rendering application, the rendering application for forwarding the digital content to an ultimate destination by way of a path therebetween, the path being defined by at least one module, the digital content initially being in an encrypted form, the method comprising:

performing an authentication of at least a portion of the path to determine whether each defining module thereof is to be trusted to appropriately handle the digital content passing therethrough;

decrypting the encrypted digital content if in fact each such defining module is to be trusted; and

forwarding the decrypted digital content to the rendering application for further forwarding to the ultimate destination by way of the authenticated path.

25. The method of claim 24 wherein the path includes a user mode portion and a kernel portion, the method further comprising:

scrambling the digital content upon such digital content being outputted from the rendering application to the path such that the scrambled digital content enters the user mode portion of the path, such scrambled digital content then passing through the modules that define the user mode portion of the path and transiting from the user mode portion to the kernel portion of the path; and

de-scrambling the scrambled digital content upon such scrambled

digital content transiting from the user mode portion to the kernel portion.

26. The method of claim 25 comprising de-scrambling the scrambled digital content by way of a de-scrambling module.

27. The method of claim 25 comprising de-scrambling the scrambled digital content in the kernel portion of the path.

28. The method of claim 27 comprising performing an authentication of at least a portion of the kernel portion of the path to determine whether each defining module thereof is to be trusted to appropriately handle the digital content passing therethrough.

29. The method of claim 24 wherein the path includes a user mode portion and a kernel portion, the method comprising performing an authentication of at least a portion of the kernel portion of the path to determine whether each defining module thereof is to be trusted to appropriately handle the digital content passing therethrough.

30. The method of claim 29 further comprising:

scrambling the digital content upon such digital content being outputted from the rendering application to the path such that the scrambled digital content enters the user mode portion of the path, such scrambled digital content then passing through the modules that define the user mode portion of the path and transiting from the user mode portion to the kernel portion of the path; and

de-scrambling the scrambled digital content upon such scrambled digital content transiting from the user mode portion to the kernel portion.

31. The method of claim 30 comprising de-scrambling the scrambled digital content by way of a de-scrambling module.

32. The method of claim 30 comprising de-scrambling the scrambled digital content in the kernel portion of the path.

33. The method of claim 24 wherein performing the authentication comprises:

traversing the at least a portion of the path to develop a map of each module in the path; and

authenticating each module in the map.

34. The method of claim 33 wherein performing the authentication further comprises ignoring each module not in the map.

35. The method of claim 24 wherein performing the authentication comprises:

authenticating an initial module;

determining all first destination modules that receive data from such initial module;

authenticating each such first destination module;

determining all second destination modules that receive data from each such first destination module;

iteratively repeating the authenticating and determining steps for third, fourth, fifth, etc. destination modules until each module in such at least a portion of the path has been determined and authenticated.

36. The method of claim 35 wherein authenticating the initial module comprises authenticating a module in the at least a portion of the path that is to receive the digital content before any other module in the at least a portion of the path, whereby the initial module leads to fully determining all other modules that define the at least a portion of the path.

37. The method of claim 35 comprising employing a database device to keep track of all modules determined to be in the at least a portion of the path, whereby already-determined modules in the at least a portion of the path can be recognized.

38. The method of claim 24 wherein performing an authentication comprises:

for each module in the at least a portion of the path:

receiving from the module a certificate as issued by a certifying authority; and

determining from the received certificate whether such received certificate is acceptable for purposes of authenticating the module.

39. The method of claim 38 wherein performing an authentication further comprises checking a revocation list to ensure that the received certificate has not been revoked.

40. The method of claim 39 further comprising:

receiving the revocation list from a certifying authority;

storing the received revocation list in a secure location.

41. The method of claim 38 wherein performing an authentication further comprises refusing to decrypt the encrypted digital content if at least one module in the at least a portion of the path fails to provide an acceptable certificate.

42. The method of claim 38 wherein performing an authentication further comprises decrypting the encrypted digital content if all the modules in the at least a portion of the path provide an acceptable certificate.

43. The method of claim 38 wherein performing an authentication further comprises, for each module in the at least a portion of the path that fails to provide

an acceptable certificate:

defining a sub-portion of the path including the non-providing module;

scrambling the digital content upon such digital content entering the sub-portion of the path, such scrambled digital content then passing through the modules that define the sub-portion of the path; and

de-scrambling the scrambled digital content upon such scrambled digital content exiting from the sub-portion of the path; and

declaring the sub-portion trustworthy.

44. The method of claim 24 wherein the path includes a user mode portion and a kernel portion, the method comprising performing an authentication of the user mode portion of the path and of the kernel portion of the path to determine whether each defining module thereof is to be trusted to appropriately handle the digital content passing therethrough.

45. The method of claim 24 wherein the path includes a tunneled portion, the method further comprising:

scrambling the digital content upon such digital content entering the tunneled portion of the path, such scrambled digital content then passing through the modules that define the tunneled portion of the path; and

de-scrambling the scrambled digital content upon such scrambled digital content exiting from the tunneled portion of the path;

and wherein performing an authentication comprises performing an authentication of at least a portion of the path external to the tunneled portion of the path to determine whether each defining module thereof is to be trusted to appropriately handle the digital content passing therethrough, an authentication of the tunneled portion being unnecessary.

46. The method of claim 45 wherein the path includes a user mode

portion, a kernel portion, and a tunneled portion in the user mode portion, the method further comprising:

scrambling the digital content upon such digital content entering the tunneled portion of the user mode portion of the path, such scrambled digital content then passing through the modules that define the tunneled portion of the user mode portion of the path; and

de-scrambling the scrambled digital content upon such scrambled digital content exiting from the tunneled portion of the user mode portion of the path.

and wherein performing an authentication comprises performing an authentication of at least a portion of the path external to the tunneled portion of the user mode portion of the path to determine whether each defining module thereof is to be trusted to appropriately handle the digital content passing therethrough, an authentication of the tunneled portion being unnecessary.